This document of "things to do" and instructions will help prepare your organization to use the Enterprise Invoice/Service Management (EIM/ESM) business service within the Virtual Gateway.

Please find below a summary checklist of requirements that we ask you to complete in this document.

> ❑   **1.** Read and Sign the Virtual Gateway Services Agreement **(FORM A)**.
>
> ❑   **2.** Read and Sign the EOHHS Virtual Gateway Designation of Access Administrator Form **(FORM B)**.
>
> ❑   **3.** Read and Sign the Enterprise Invoice/Service Management Rider **(FORM C)**.
>
> ❑   **4.** Read and Complete the Organization Management Form **(FORM D)**.
>
> ❑   **5.** Read and Complete the User Request Forms.
>
> ❑   **6.** Return completed Welcome Package Forms and Agreements to EOHHS Virtual Gateway Operations.

The rest of this document explains in detail the documents we ask you to complete. Before "going live" on EIM/ESM, each organization will need to:

1.   READ AND SIGN THE VIRTUAL GATEWAY SERVICES AGREEMENT (FORM A)

The *EOHHS Virtual Gateway Services Agreement* sets forth the terms and conditions to which your organization must agree in order to access the Virtual Gateway. The *EOHHS Virtual Gateway Services Agreement* must be signed by an individual at your organization who has the legal authority to sign on behalf of your organization, as evidenced by your organization's charter or bylaws.

2.   READ AND SIGN THE EOHHS VIRTUAL GATEWAY DESIGNATION OF ACCESS ADMINISTRATOR FORM (FORM B)

Each organization must designate an individual to be their Virtual Gateway Access Administrator. This 'Access Administrator' is the liaison between EOHHS and the organization and its users for issues relating to Virtual Gateway account information and access. Specifically, the Virtual Gateway Access Administrator is responsible for approving, modifying, or removing user access privileges to any of the Virtual Gateway's business services for employees in your organization. The *EOHHS Virtual Gateway Designation of Access Administrator Form* must be signed by an individual at your organization who has the legal authority to sign on behalf of your organization, as evidenced by your organization's charter or bylaws.

3. READ AND SIGN THE ENTERPRISE INVOICE MANAGEMENT/ENTERPRISE SERVICE MANAGEMENT RIDER (FORM C)

Certain business services require organizations to agree to additional terms and conditions of use, which are included in riders to the standard Virtual Gateway Services Agreement. These riders must also be signed by your organization, and will become incorporated into the Virtual Gateway Services Agreement.

4. COMPLETE THE SECURITY FORMS

The EIM/ESM Implementation Team will hold workshops and conference calls to assist providers in completing the Security Forms. An initial schedule of workshops and calls is provided in the Welcome Package. If you need information on the schedule for these workshops and calls, please call Virtual Gateway Customer Service at 1-800-421-0938. We understand that this is a lot of information. Please call us for help if you need it!

4.1 Security Overview

Enterprise Invoice/Service Management (EIM/ESM) is a web-based service, which means it can be accessed from anywhere. As a result, special steps have to be taken to ensure that the data stored within it is secure and accessible only to those who are authorized to have such access. Unlike paper copies of invoices, contracts, client rosters etc. that can be locked in a filing cabinet, the online copies have to be secured electronically – this is done via a combination of *Organization Management, Security Roles*, and *Data Access* rules.

An **Organization** is a legal entity or location that users are associated with. It can be a parent corporation, a site office where services are rendered (e.g., group home) or where billing occurs (e.g., regional billing office). *This is the information documented on the Organization Management Form (Form D).* Organizations in EIM/ESM can be divided into sub-organizations, with staff members employed at the appropriate levels. A sub-organization is a site that has a direct relationship to a parent organization – i.e., it is *owned and operated* by the parent organization. For example, a provider organization can have multiple facilities or sites where services are delivered. **An organization should be documented on the form if it meets at least one of the following criteria:**

- EIM/ESM will be accessed there
- Clients are enrolled there
- Clients receive services there (excluding personal homes of clients)

A **User** is an individual associated with one or more organizations who will have access to the system in order to complete their job duties.

Security Roles define the user's business functions in the system and control what the user can and cannot *do* in EIM/ESM. *This is the information documented on the User Request Form (URF).* For example, the "Invoice Reviewer" security role enables the individual to review invoices in the system, but they cannot create or edit them. The user must be assigned the "Invoice Manager" role to be able to create and edit invoices. A user can have more than one security role and a security role can be associated with more than one user. A user should be assigned only the roles relevant to his or her job function. A user associated with any site will have access to data associated with all the sites below that site.

Data Access rules control what the user can and cannot *see* in EIM/ESM. The data access rules that are predefined in the system consider the user's organizational relationship to control what data records a user

has access to see. For example, the data access rules will ensure that an "Invoice Reviewer" can review invoices for his/her organization and the various organizations under it, but cannot view invoices for other provider organizations. This is the way the Organization Management Form (Form D) and the URF are connected.

The combination of organization management structures, security roles, and data access rules secure the EIM/ESM service so users perform only the system functions that they are authorized to perform, and see only the specific data records that they are authorized to see. To that end, it is necessary that the organization structure and security roles are thoughtfully coordinated to permit appropriate access to system functionality and data. We recommend that you review the URF instructions (4.4) before completing the Organization Management Form. This will give you a better understanding of how the two forms relate to each other.

4.2 <u>Organization Management Form</u> (FORM D)

This form identifies the main (parent) provider organization and whether that organization has multiple sites under it (sub-organizations). The hierarchical relationship between these sites is relevant to how security roles are eventually assigned within the EIM/ESM service. Organizations not affiliated with EIM/ESM users (IT, Administration etc.) will not have to be part of this Organization Management Template.

4.2.1   *Completing the Organization Management Form*

You will need to complete one organization management form for your organization. This form should be completed comprehensively, i.e. it should reflect the entire provider organization as it pertains to all Purchase of Service EOHHS contracts. The vast majority of the organization management effort occurs in preparation for the first time a provider goes live with the EIM/ESM service. If and when a provider goes live again with additional contracts, the organization management structure can be revisited for validation. Nonetheless, it is important that the provider organization structure be captured accurately, and in its entirety, the first time it is completed, because it will serve as the foundation for security access.

The first step to compiling accurate and complete information is to identify people who can validate the organization management structure for your organization and its affiliates. These people will then need to:

- Document the structure of your organization, identifying your "parent" organization and then all of its sub-organizations (as many tiers as needed). As mentioned earlier, a sub-organization is a site that has a direct relationship to a parent organization – i.e., it is *owned and operated* by the parent organization. Furthermore, a sub-organization should be documented if EIM/ESM will be accessed there, clients are enrolled there, or services are delivered there (excludes personal homes of clients). In addition, you may create sub-organizations at one physical location to separate security access. (See Figure 1, Tier 2 for an example)

- List all affiliates. Affiliates will include organizations that may deliver services, enroll clients, or perform billing on your behalf, but are *NOT owned and operated* by your parent organization. Note that information on affiliates is *only necessary if:*
  - ✓ you wish to have staff at affiliate organizations access EIM/ESM directly
  - ✓ clients are directly enrolled in those organizations
  - ✓ clients receive services at those affiliate locations

The rest of this section explains in detail the information needed to complete the Organization Management Form.
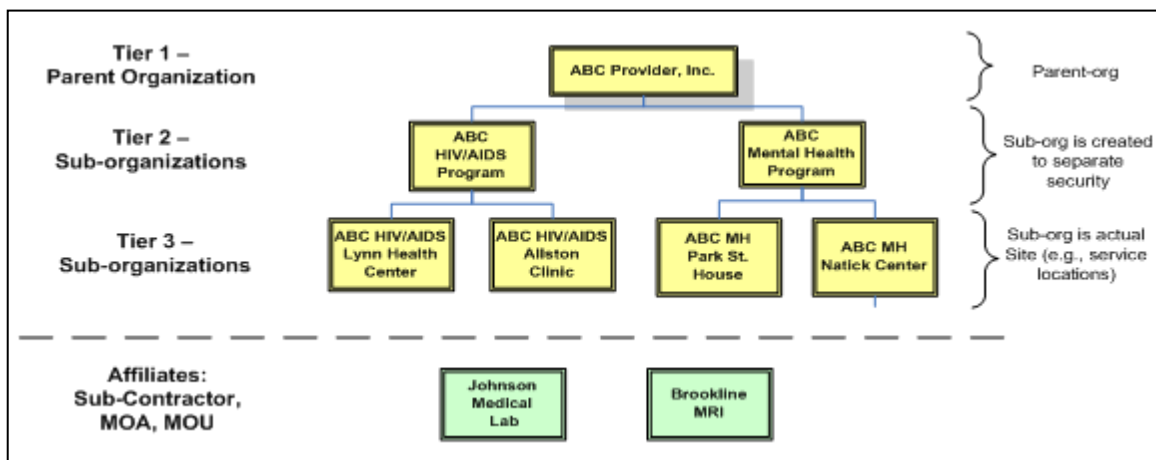
Tips:

Prior to completing the form, we recommended that you develop or verify your Organization Chart that represents your organization's structure. A sample chart is included in Figure 1 (This is represented in Example 1 on the form):

Figure 1

Field-by-field Instructions:

The underline first line of the sheet is for your Parent organization's information. The rest are for the sub-organizations and affiliates (if applicable).

Name* – In the case of the overall parent organization, this is the official name of your organization (e.g., ABC Provider, Inc). In the case of sub-organizations, please precede this with the short name of the immediate parent org (e.g., ABC Mental Health if it is the Mental Health Program, ABC HIV/AIDS, if it is the HIV/AIDS program).

Short Name* – The abbreviated, or "doing business as" name for your organization (e.g., ABC if it is ABC Provider Inc, ABC HIV/AIDS if it is ABC HIV/AIDS program).

Parent Organization or Affiliate – Complete this field for sub organizations and affiliates as follows:

- **Sub-organizations:** If you indicate an organization is a sub-organization, please include the *immediate* parent organization's short name in this column. An immediate parent is the organization that is one level above the sub-organization being described (e.g., ABC HIV/AIDS is the immediate parent of ABC HIV/AIDS Lynn Health Center).
- **Affiliates:** If you indicate an organization is an affiliate with whom you subcontract, please mark the column with 'Affiliate'. Once again, information on affiliates is only necessary if you wish to have staff at your affiliate organizations access EIM/ESM directly, clients are directly enrolled in those organizations, or clients receive services at those affiliate locations.

Affiliate Type – If you indicated that an organization is an "Affiliate", select what your contract relationship is with that provider: Sub-contractor, Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU).

VCC # – Provide your vendor code (VCC#). You only need to complete the VCC on the parent line of the template (e.g., ABC Provider, Inc.).

Address Line 1* – Street address or P.O. Box

Address Line 2* – Additional information such as suite number or floor number

City – self-explanatory

State – self-explanatory

Zip Code – five digit code

*Note:
- Legal Name and Short Name have a 35 Character Limit
- Address Line 1& 2 have a *combined* 30 Character Limit
- Punctuation and symbols (e.g. # . ,) are not permitted throughout the form

4.2.2 Return the Completed Form to the Virtual Gateway Operations Team

- Save the completed form by adding your parent organization's **short name** and the **date** (MMDDYY) to the end of the filename (e.g., *EIM Org Mgt Structure Example and Form – ABC 052507.xls*)
- Return the form to Virtual Gateway Operations via email at virtualgatewaydeployment@state.ma.us

4.3 User Request Forms (URFs)

Once the Organization Management Form is complete, the URFs are used to identify specific individuals who will be using the EIM/ESM service at *each* of the organizations and sub-organizations identified in the Organization Management Form and assign them security roles that correspond to their job function. The URFs are used to add, change, or delete individual user account information for EIM/ESM access through the Virtual Gateway. The Virtual Gateway will use this information to create an appropriate login (username and password) for the personnel who will be using the EIM/ESM service.

Additionally, URFs will identify who needs training and their training course requirements. Training is mandatory for all EIM/ESM users prior to Go-Live. Training details will be provided in a later communication. The earlier the URFs are submitted, the earlier users will be able to register for training.

4.3.1 Completing the User Request Forms

You will need to complete **one URF for each organization and sub-organization** where users are assigned. The steps for completing the URFs and assigning security roles are as follows:

- **Step One:** Complete the Organization Management form.

- **Step Two:** For the relevant contracts, you will identify specific individuals who will be using the EIM/ESM service at *each* of the organizations and sub-organizations identified on your Organization Management Form. Please note the following points when completing URFs:

  - Only staff that will be directly accessing EIM/ESM will need to be identified.

- A staff person associated with any site will have access to data associated with all the sites below that site.

- If a staff person works at multiple sites, they will have to be included on the URF for each of those sites separately, or be included on the URF of a parent site, where they will have access to all sites associated with the organization.

- It is very important that the organization's name is recorded, as it is listed under the "Name" column under the Organization Management Form (Form D), on each URF (there is a space for this on the bottom of the URF). The org name can refer to the parent organization or to any of the sub-organizations under it.

- **Step Three**: On the URF complete the following information for each user:

    1. Full name (first name, last name and if applicable middle initial)

    2. Four Digit PIN Number

    3. Month and day of birth

    4. Work e-mail address

    5. Work phone number

- **Step Four**: For each user listed you will need to assign specific roles according to their business functions. Please follow the guidelines below when assigning roles.

    o A user must have at least one role assigned to them, but in most cases it will be more than one. ***Note: Please refer to the Role Guide tab of the URF for a complete list of the roles, their definitions, and specific required roles. (A copy of the Role Guide is included at the end of this document.)***

    o Remember, users should only be able to access functionality applicable to their job function. However, you must also ensure that users can perform their job function without limitation.

For each **role** assigned, select from the pick list labeled 'Existing Role', 'Delete Role', or 'Add Additional Role' according to the following definitions:

    o **Existing Role –** Designates existing user role assignments in EIM/ESM.

    o **Add Additional Role –** Designates additional user role assignments in EIM/ESM. *If this is your first time completing the URF, please select the 'Add Additional Role' pick option for all users.*

    o **Delete Role –** Deactivates an existing user role assignment in EIM/ESM.

- **Step five**: For each **user**, check the appropriate box (one only) in the columns labeled 'New', 'Modify', or 'Deactivate' according to the following definitions:

    o **New User –** Designates first time user role assignments and initiates the creation of a new security account. *If this is your first time completing the URF, please check the 'New' box for all users.*

    o **Modify Existing User –** Modifies an existing user's security roles by assigning additional roles or removing existing roles. The 'Modify' box can be used in the future to indicate that the roles that are assigned to a user need to be changed.

     o **Deactivate Existing User –** Deactivates an existing user's security account and all of its associated roles. The 'Deactivate' box can be used to indicate that a staff member is no longer employed by an organization or if the employee's job changes and the person no longer uses EIM/ESM. (the user will no longer be able to access the system).

4.3.2   Return the Completed Form to the Virtual Gateway Operations Team

- Save the completed URF by adding the applicable parent or sub organization's **short name** and the **date** (MMDDYY) to the end of the filename (e.g., *user_request_form– ABC 052507.xls*).
- Return the form to Virtual Gateway Operations via email at virtualgatewaydeployment@state.ma.us.
- No wet signature is needed to submit the form to Virtual Gateway Operations. However, you must keep a copy of each URF, signed by the Access Administrator, within your organization's records.

5. RETURN COMPLETED WELCOME PACKAGE FORMS AND AGREEMENTS TO EOHHS VIRTUAL GATEWAY DEPLOYMENT

Please mail the original executed *Virtual Gateway Services Agreement (FORM A), EOHHS Virtual Gateway Designation of Access Administrator Form (FORM B)*, and *EIM/ESM Rider (FORM C)* to the following address:

> **EOHHS Virtual Gateway Operations – IDM Operations**
> **100 Hancock Street, 5th Floor**
> **Quincy, MA 02171**

Please email the *Organization Management Form (FORM D)* and *URF Forms* to:

> **EMAIL: virtualgatewaydeployment@state.ma.us**

For additional information on the EIM/ESM service, visit www.mass.gov/vg/eimesm   You will the find Newsletters, the EIM/ESM Fact Sheet, Frequently Asked Questions (FAQs), training information, and the Virtual Gateway System Requirements available for download.

In the meantime, if you have any questions or need additional assistance, please do not hesitate to contact Virtual Gateway Customer Service at 1-800-421-0938.

Sample User Request Form Role Guide (refer to the Role Guide tab of the URF for the latest version)

Common Roles				
Contract and Payment Reviewer Roles	Title	**Contract and Payment Reviewer (Applicable to all CR, UR, and AR Contracts)**		
	Description	Ability to Review Contract Data Including Amounts, Balances, Rates, Line Item Budgets, etc. Ability to Review and Track Payment Information View Relevant Reports and Invoices		
Manage Locations	Title	**Manage Locations (Applicable to all CR, UR, and AR Contracts)**		
	Description	Ability to manage Participating Organizations on a contract. Ability to update locations for enrollments.		
EIM ROLES				
	Contract Type	**Cost Reimbursement (CR)**	**Unit Rate (UR)**	**Accommodation Rate (AR)**
Billing Roles	Title	**CR Billing**	**UR Billing**	**AR Billing**
	Description	Create CR Invoice / Supplementals Enter invoice data Release Invoices for Internal Approval View Relevant Reports and Invoices Ability to Include SDRs with Invoices Ability to Include Invoice Assessments with Invoices	**Centralized Billing Model:** Create SDR / Supplementals Enter SDR Data Release SDR for Internal Approval View Relevant Reports and Invoices **Decentralized Billing Model:** Create SDR / Supplementals at the Site Level Release SDR for Internal Approval Enter SDR Data View Relevant Reports and Invoices	Create AR Invoice / Supplementals Release AR Invoice for Internal Approval Enter AR SDR Data Review Relevant Reports and Invoices
	If Applicable	N/A	Claim Reviewer for HIPAA	N/A
Authorizer Roles	Title	**CR Authorize**	**UR Authorize**	**AR Authorize**
	Description	Ability to Authorize Invoices / Supplementals to the Agency for Payment View Relevant Reports and Invoices Ability to Review Associated SDRs Ability to Review Associated Invoice Assessments	Ability to Authorize SDRs / Supplementals to the Agency for Payment Release SDR for Internal Approval View Relevant Reports and Invoices	Ability to Authorize AR Invoices to the Agency for Payment Ability to review associated AR SDR Review Relevant Reports and Invoices
	If Applicable	N/A	Claim Reviewer for HIPAA	N/A
Releasing Role	Title	**CR**	**UR Release**	**AR**
	Description	N/A	Ability to Release SDRs and Supplementals to the Agency for Payment Release SDR for Internal Approval View Relevant Reports and Invoices	N/A
Managing Role	Title	**HIPAA Claim Manager**		
	Description	Allows users to review, correct, and void claims Allows users the privilege to review clients and client names in ESM		
Viewing Roles	Title	**CR Review**	**UR Review**	**AR Review**
	Description	View Only Access to Invoices View Relevant Reports and Invoices Ability to Review Associated SDRs Ability to Review Associated Invoice Assessments	View Only Access to SDRs View Relevant Reports and Invoices	View Only Access to the AR Invoice and AR SDR Review Relevant Reports and Invoices
	If Applicable	N/A	Claim Reviewer for HIPAA	N/A
ESM ROLES				
Consent Manager	Description	Ability to grant electronic consents for the release of individual client information		
Client Data Manager	Description	Manage client information, referrals and enrollments Create, update, and review enrollment and disenrollment assessment data Manage professional service records, service plans, notes and tasks, and final diagnosis results Create and edit service plans, diagnosis assessment, and screening assessment data View relevant reports		
Client Data Reviewer	Description	Review client information, referrals and enrollments Review enrollment and disenrollment assessment data Review service plans, diagnosis assessment, and screening assessment data View relevant reports		
SBHC ESM Reports	Description	View reports associated with DPH School Based Health Program, including the Encounter Status Report, Aggregate Enrollment Status, Aggregate Service Report, Aggregate Diagnosis Report, and Diagnosis Report		